ELSEVIER
Theoretical Computer Science 143 (1995) 335–342
Theoretical Computer Science

Note

A nonlinear lower bound on the practical combinational complexity☆

Xaver Gubáš[a], Juraj Hromkovič[b,*], Juraj Waczulík[c]

[a]*Department of Computer Science, Comenius University, 842 15 Bratislava, Slovak Republic*
[b]*Institut für Informatik und Praktische Mathematik, Christian-Albrechts-Universität zu Kiel, Olshausenstraße 40, 24098 Kiel, Germany*
[c]*Computer Science Institute of the Comenius University, 842 15 Bratislava, Slovak Republic*

Received August 1992; revised October 1994
Communicated by M.S. Paterson

Abstract

An infinite sequence $F = \{f_n\}_{n=1}^{\infty}$ of one-output Boolean functions with the following two properties is constructed:

(1) f_n can be computed by a Boolean circuit with $O(n)$ gates.

(2) For any positive, nondecreasing, and unbounded function $h: N \to R$, each Boolean circuit having an $m/h(m)$ separator requires a nonlinear number $\Omega(nh(n))$ of gates to compute f_n (e.g., each planar Boolean circuit requires $\Omega(n^2)$ gates to compute f_n).

Thus, one can say that f_n has linear combinational complexity and a nonlinear practical combinational complexity because the constant-degree parallel architectures used in practice have separators in $O(m/\log_2 m)$.

1. Introduction

One of the most challenging problems in complexity theory is to prove a nonlinear lower bound on the combinational complexity (the number of gates in Boolean circuits) of a specific Boolean function. The highest lower bounds are only linear ones (for the base of all Boolean functions of two variables in [2, 5, 6, 11, 21, 24], for some special complete bases in [22, 24, 27]) despite the well-known fact that almost all Boolean functions of n variables require $\Omega(2^n/n)$ combinational complexity [17, 26].

☆Supported in part DFG-Grant DI 412/2-1 and by the Leibniz program of DFG.
*Corresponding author.

SSDI 0304-3975(94)00269-X

One attempt to attack this challenging problem has been in the development and application of the information transfer technique (communication complexity) (see, for instance [1, 7–9, 13, 16, 20, 28, 29, 31]). This technique has been successfully applied for proving lower bounds on the number of gates of planar Boolean circuits and the layout area of Boolean circuits, using the Planar Separator Theorem of Lipton and Tarjan [14]. One extension of the application for planar circuits was made in [10], where it has been shown that each unbounded fan-in, fan-out Boolean circuit with a $O(m^a)$ vertex-separator for an $a < 1$ must have $\Omega(n^{1/a})$ processors (gates) to compute some specific one-output Boolean functions. The above-mentioned result has led to the formulation of the following two research problems.

1. To improve the result proved in [10] by proving a nonlinear lower bound on the number of gates of Boolean circuits with $O(m/f(m))$ separators for some functions $f(m)$ increasing slower than m^a for any $a > 0$.

2. To decide whether there exists a one-output Boolean function with a linear combinational complexity and a nonlinear "practical" combinational complexity, where the practical combinational complexity of a Boolean function f is the minimum over the combinational complexities of all Boolean circuits with sublinear separators computing f.

The importance of problem 2 (for which the positive answer is expected) consists in the fact that the existence of such a Boolean function implies that a strongly connected topology (for example, magnifiers [4]) brings additional computing power to circuits (parallel architectures). On the other hand the existence of such a Boolean function also means that there are functions which are theoretically easy to compute (with a linear number of gates) but which are not easy (a nonlinear number of gates is required) for any parallel architecture currently used, because the circuits and the architectures used in practice usually have separators in $O(m/\log m)$.

The main result of this paper gives the solution of both problems 1 and 2 by constructing an infinite sequence $F = \{f_n\}_{n=1}^{\infty}$ of one-output Boolean functions with the following two properties:

(i) f_n can be computed by a Boolean circuit with $O(n)$ gates, i.e. $\{f_n\}_{n=1}^{\infty}$ has a linear combinational complexity,

(ii) for any positive, nondecreasing and unbounded function $h: N \to R$, each Boolean circuit having an $m/h(m)$ separator requires a nonlinear number $\Omega(n \cdot h(n))$ of gates to compute f_n.

An interesting consequence of this result is that we construct a function with a linear combinational complexity and a quadratic planar complexity (see [18, 19, 30, p. 344] for the definition of planar Boolean circuits and [15] for the fact that planar graphs of m nodes have $O(\sqrt{m})$ separators). Moreover this result explicitly shows the limit of information transfer techniques [8, 10, 13, 15, 16, 23, 31] for proving circuit lower bounds.

This paper is organized as follows. In the next section we give the construction of a special sequence of Boolean functions F with linear communication complexity. In Section 3 it is shown that F has linear combinational complexity (i.e. that F has the

property (i)). The lower bound (ii) for computing $F = \{f_n\}_{n=1}^{\infty}$ is proved in Section 4 by showing that each Boolean function with linear communication complexity requires a nonlinear number of gates to be computed by Boolean circuits with sublinear separators.

2. Construction of F

To construct $F = \{f_n\}_{n=1}^{\infty}$ we use a result of several authors (see, for example [4]) providing a constructive proof of the magnifiers among 3-regular graphs. Thus, we can assume that there are a positive constant c and an algorithm which for a given even positive integer $n \geqslant 6$ constructs a graph $G_n = (V_n, E_n)$ with the following three properties:

(i) G_n is a 3-regular graph,

(ii) $|V_n| = n$,

(iii) For each $X \subseteq V_n$, $|X| \leqslant n/2$ there are at least $c \cdot |X|$ edges between the vertices in X and the vertices in $V_n - X$.

Now, we use a construction similar to the construction of Lipton and Sedgewick [13] in order to construct $f_n: \{0,1\}^n \to \{0,1\}$ from G_n. We note that each 3-regular graph with at least six vertices is 3-colourable (Brook's Theorem [3]) which is used for the following construction.

The construction of f_n from $G_n = (V_n, E_n)$ is done in the following four steps.

1. Denote the n vertices of G_n by n variables $x_1, x_2, \ldots, x_n$ in an arbitrary way.

2. Colour the vertices of G_n using 3 colours $\bar{1}, \bar{2}, \bar{3}$ by giving a function $h: V_n \to \{\bar{1}, \bar{2}, \bar{3}\}$ with the property $h(r) \neq h(s)$ for each $(r,s) \in E_n$.

3. For all $i, j \in \{1,2,3\}, i < j$, define

$$f_n(i,j) = \bigwedge_{(u,v) \in E_{i,j}} (u \vee v),$$

where

$$E_{i,j} = \{(u,v) | (u,v) \in E_n \wedge h(u) = \bar{i} \wedge h(v) = \bar{j}\}.$$

4. Define $f_n(x_1, \ldots, x_n) = f_n(1,2)(x_1, \ldots, x_n) \vee f_n(1,3)(x_1, \ldots, x_n) \vee f_n(2,3)(x_1, \ldots, x_n)$.

Note, that f_n is a monotone function. We have defined f_n only for even n, but one can extend the definition for odd n's in several distinct ways. For instance, $f_{n+1}(x_1, \ldots, x_{n+1}) = f_n(x_1, \ldots, x_n) \vee x_{n+1}$.

Now, we shall show that the function f_n constructed in the way described above has linear information content. We shall use this fact later to show that a nonlinear number of gates is required to compute F on circuits with sublinear separators.

We give the definition of Ullman [29] to explain what "f_n has the information content $I(f_n)$" means. Let $X = \{x_1, \ldots, x_n\}$, and let $P_X = \{\Pi_X = (X_L, X_R) | X_L \cap X_R = \emptyset, X = X_L \cup X_R, \lfloor n/3 \rfloor \leqslant |X_L| \leqslant |X_R|\}$ be the set of all *almost balanced partitions* Π_X of X. For each word $a = a_1 a_2 \ldots a_n \in \{0,1\}^n$ and for each almost balanced partition

$\Pi_X = (\{x_{i_1}, x_{i_2}, \ldots, x_{i_r}\}, \{x_{j_1}, x_{j_2}, \ldots, x_{j_s}\})$ (note that $r+s=n$), $\Pi_X(a,L) = a_{i_1}a_{i_2}\ldots a_{i_r}$, $\Pi_X(a,R) = a_{j_1}a_{j_2}\ldots a_{j_s}$, and $\Pi_X^{-1}(\Pi_X(a,L), \Pi_X(a,R))$ denotes the original word a. A *fooling set for Π_X and f_n* is any set $S(\Pi_X, f_n) \subseteq \{0,1\}^n$ having the following two properties:

1. For every two words $a, b \in S(\Pi_X, f_n)$: $f_n(a) = f_n(b)$.
2. For every two words $a, b \in S(\Pi_X, f_n)$:

$$f_n(a) \neq f_n(\Pi_X^{-1}(\Pi_X(a,L), \Pi_X(b,R))) \quad \text{or} \quad f_n(a) \neq f_n(\Pi_X^{-1}(\Pi_X(b,L), \Pi_X(a,R))).$$

The *information content of f_n according to Π_X* is

$$I(\Pi_X, f_n) = \log_2(\max\{|S(\Pi_X, f_n)| \mid S(\Pi_X, f_n) \subseteq \{0,1\}^n \text{ is a fooling set for } \Pi_X \text{ and } f_n\}).$$

The *information content of f_n* is

$$I(f_n) = \min\{I(\Pi_X, n) \mid \Pi_X \in P_X\}.$$

The information content of languages (sequences of Boolean functions) was successfully used to prove lower bounds on the area complexity and on the area-time squared complexity of VLSI circuits. We note that the detailed description of information content as a complexity measure and its relation to communication complexity and to other complexity measures for VLSI computations can be found in [8, 9, 29].

Now, let us show that the information content $I(f_n)$ of f_n constructed from the graph $G_n = (V_n, E_n)$ is in $\Omega(n)$. Let $\Pi_X = (X_L, X_R)$ be an almost balanced partition of $X = (x_1, \ldots, x_n)$, $n \geqslant 10000 \cdot c^{-1}$.

Let $E_n(\Pi_X) = E_n \cap (X_L \times X_R)$. Obviously, the property (iii) of G_n implies that $E_n(\Pi_X) \geqslant c \cdot \lfloor n/3 \rfloor$. Now, we can assume there are $i,j \in \{1,2,3\}$, $i \neq j$, such that the number $d(n)$ of edges $(x_{r_1}, x_{s_1}), \ldots, (x_{r_{d(n)}}, x_{s_{d(n)}})$ leading between X_L and X_R and coloured by the colours $\bar{i}$ and $\bar{j}$ (either x_{r_k} is coloured by $\bar{i}$ and x_{s_k} by $\bar{j}$ for each $k \in \{1, \ldots, d(n)\}$ or x_{r_k} is coloured by $\bar{j}$ and x_{s_k} is coloured by $\bar{i}$ for each $k \in \{1, \ldots, d(n)\}$) is at least $c \cdot \lfloor n/3 \rfloor/6$. Thus, we can write

$$f_n(i,j) = \bigwedge_{k=1}^{d(n)} (x_{r_k} \vee x_{s_k}) \wedge f'_n(i,j),$$

where $f'_n(i,j) = \bigwedge_{(u,v) \in \dot{E}_{i,j}} (u \vee v)$ for $\dot{E}_{i,j} = E_{i,j} - \{(x_{r_1}, x_{s_1}), \ldots, (x_{r_{d(n)}}, x_{s_{d(n)}})\}$.

Set $A_L = (x_{r_1}, \ldots, x_{r_{d(n)}}) \in (X_L)^{d(n)}$ and $A_R = (x_{s_1}, \ldots, s_{s_{d(n)}}) \in (X_R)^{d(n)}$. Let $\bar{X}_L \subseteq X_L (\bar{X}_R \subseteq X_R)$ be the set of all distinct variables in the vector $A_L (A_R)$. Let $X'_L \subseteq \bar{X}_L$ and $X'_R \subseteq \bar{X}_R$ be subsets of the set of input variables such that for $\forall x, z \in X'_L$, $\forall y, w \in X'_R$ ($(x,y) \in E_n(\Pi_X)$ and $(z,w) \in E_n(\Pi_X)$) implies that $(x,w) \notin E_n(\Pi_X)$ and $(z,y) \notin E_n(\Pi_X)$. (Note, that X'_L and X'_R are chosen in such a way that the subgraph spanned by $X'_L \cup X'_R$ consists of independent edges.) Taking X'_L and X'_R as large as possible we have $b(n) = |X'_L| = |X'_R| \geqslant d(n)/13 \geqslant c \cdot \lfloor n/3 \rfloor/78$. (To see this consider the situation when one adds one edge (z_1, z_2) to $X'_L \times X'_R$. Then to secure the above-stated property one has to remove from $\bar{X}_L \times \bar{X}_R$ all (at most 12) edges

connected with all (at most 4) vertices adjacent to z_1 and z_2.) Let $X'_L = \{x_{u_1}, \ldots, x_{u_{b(n)}}\}$ and $X'_R = \{x_{v_1}, \ldots, x_{v_{b(n)}}\}$. Thus, we can write

$$f_n(i,j) = \bigwedge_{k=1}^{b(n)} (x_{u_k} \vee x_{v_k}) \wedge \tilde{f}_n(i,j) \wedge f'_n(i,j),$$

for some conjuction of elementary disjunctions $\tilde{f}_n(i,j)$. Now, we describe the construction of the fooling set $S(\Pi_X, f_n)$ for Π_X and f_n as a subset of $\{0,1\}^n$ in the following stages:

(1) Choose four variables y_1, y_2, y_3, y_4 from X such that $y_1 = y_2 = y_3 = y_4 = 0$ implies $f_n(k,l) = 0$ for each $(k,l) \neq (i,j)$, $k, l \in \{1,2,3\}$, $k < l$ and $y_1 = \cdots = y_4 = 0$ does not imply $f_n(i,j) = 0$. Fix the zero values of y_1, y_2, y_3, y_4 in all words in $S(\Pi_X, f_n)$.

(2) Fix the value 1 for all variables in $X' = X - (X'_L \cup X'_R \cup \{y_1, \ldots, y_4\})$.

(3) The variables in $X'_L \cup X'_R$ may have both values 0 and 1 with the following restrictions: For all $k \in \{1, \ldots, b(n)\}$ if $x_{u_k} = 1(0)$ then x_{v_k} 0(1).

Now let us show that $S(\Pi_X, f_n)$ is a fooling set for Π_X and f_n. Stage (1) ensures that $f_n(a) = f_n(i,j)(a)$ for all $a \in S(\Pi_X, f_n)$. Stage (2) secures that $f'_n(i,j)(a) = 1$ and $\tilde{f}_n(i,j)(a) = 1$ for all $a \in S(\Pi_X, f_n)$ which implies

$$f_n(a) = \bigwedge_{k=1}^{b(n)} (a_{u_k} \vee a_{v_k}) \quad \text{for each } a = a_1 \ldots a_n \in S(\Pi_X, f_n).$$

From this fact and stage (3) we have that for all distinct $a, b \in S(\Pi_X, f_n)$ either

$$1 = f_n(a) \neq f_n(\Pi_X^{-1}(\Pi_X(a, L), \Pi_X(b, R))) = \bigwedge_{k=1}^{b(n)} (a_{u_k} \vee b_{v_k}) = 0$$

or

$$1 = f_n(a) \neq f_n(\Pi_X^{-1}(\Pi_X(b, L), \Pi_X(a, R))) = \bigwedge_{k=1}^{b(n)} (b_{u_k} \vee a_{v_k}) = 0,$$

i.e. $S(\Pi_X, f_n)$ is a fooling set.

Now let us estimate the cardinality of $S(\Pi_X, f_n)$. Since $b(n) \geqslant c \cdot \lfloor n/3 \rfloor / 78$ we have $|S(\Pi_X, f_n)| \geqslant 2^{(c \cdot \lfloor n/3 \rfloor / 78) - 4}$.

Thus we have constructed a sequence $F = \{f_n\}_{n=1}^{\infty}$ of Boolean functions with the information content $I(f_n) \in \Omega(n)$.

3. Upper bound

In this section we show that the combinational complexity of the function sequence F constructed in the previous section is linear.

Boolean circuits are considered as the usual Boolean circuits model [30] whose gates have fan-in bounded by 2 and an unbounded fan-out. The gates can realize any Boolean function of two variables. The *combinational complexity* C of Boolean circuits is taken here as the number of gates and input vertices. Usually the input vertices are

not included but this $+n$ factor is negligible for our asymptotical considerations. For any Boolean circuit B we shall denote by $C(B)$ the combinational complexity of B.

Since the number of vertices in G_n is n and the degree of G_n is bounded by 3 we have that the number of edges in G_n is at most $3n/2$. Thus, the function f_n expressed as the formula $f_n(1,2) \vee f_n(1,3) \vee f_n(2,3)$ has a linear size (i.e. it contains at most a linear number of symbols). Obviously, there is a Boolean circuit with a linear number of gates realizing f_n. We note that the fan-out of all gates is bounded by 2 and that the depth of this circuit is logarithmic (note, that if we use unbounded fan-in circuits then the depth is only three). The result of Section 4 also claims that this circuit does not have any sublinear separator.

4. Lower bound

To formulate our lower bound for F we need first to make precise the meaning of the notion "separator" used in this paper.

Definition 4.1. Let G be a graph having $n \geqslant 2$ vertices, and let $g: N \to N$ be a function. We say that G has a g-separator if there are $g(n)$ vertices in G such that their deletion divides G into two components G_1 and G_2 with the following two properties:

(a) for $i = 1, 2$, the number of vertices in G_i is at most $n/2$,

(b) for $i = 1, 2$, G_i either consists of one node or G_i has a g-separator.

If the graph G corresponds to a Boolean circuit B we say also that *the circuit B has a g-separator.*

In this section we shall prove the following result.

Theorem 4.2. *Let $h: N \to R$ be a positive, nondecreasing and unbounded function, $h(m) \leqslant m$ for all $m \in N$. Let $\{B_n\}_{n=1}^{\infty}$ be a sequence of Boolean circuits such that, for each n, B_n computes f_n and B_n has a $C(B_n)/h(C(B_n))$-separator. Then*

$$C(B_n) \in \Omega(nh(n)).$$

Proof (sketch). Since almost all the arguments used to prove this lower bound were already presented in Theorem 2.3 in [10], we give only the outline here.

Let, for any $n \in N$, B_n be a circuit computing f_n, and let G_n be the graph corresponding to B_n. Let $G_n = (V_n, E_n)$ have m vertices and an $m/h(m)$-separator. Let m be considered as the function of n of the form $m(n) = n \cdot r(n)$ for some function r. Using the same algorithm as the algorithm used in Theorem 2.3 in [10] one can divide G_n into two components $G^1 = (V^1, E^1)$ and $G^2 = (V^2, E^2)$ such that

(i) G^i contains at least $\lfloor n/3 \rfloor$ input vertices of B_n for $i = 1, 2$.

(ii) The number of removed nodes is at most

$$z(m) \leqslant m \cdot \sum_{i=0}^{\log_2 r(n)} (2^i h(m/2^i))^{-1}.$$

(Note, that the dividing procedure from [10] halves the component of G with the maximal number of input vertices while there exists a component at least $2 \cdot \lceil n/3 \rceil$ input vertices. Obviously, this procedure consists of at most $\log_2 r(n) + 1$ steps because $m(n)/2^{\log_2 r(n)+1} = n \cdot r(n)/2r(n) = n/2$ and no component of at most $n/2$ nodes can involve more than $n/2$ input nodes.)

Obviously, each vertex of B_n has at most two input edges and some number of output edges, where each transfers exactly one Boolean value during the whole computation on an input, and all output edges of the same vertex transfer the same value. So, to remove $z(m)$ nodes with their adjacent edges corresponds to the flow of at most $3 \cdot z(m)$ bits between G^1 and G^2. Thus, $3z(m) \geqslant I(f_n) \geqslant bn$ (for the formal proof of the first unequality see [10]) for some constant b and all $n \geqslant n_0$ for some constant n_0. We bound $z(m)$ as follows

$$z(m) \leqslant m \cdot (h(m/2^{\log_2 r(n)}))^{-1} \cdot \sum_{i=0}^{\log_2 r(n)} 2^{-i} \leqslant 2 \cdot m \cdot (h(m/(r(n)))^{-1} = \frac{2nr(n)}{h(n)}.$$

Since $z(m) \in \Omega(n)$ we obtain $r(n) \in \Omega(h(n))$ which completes the proof. □

Theorem 4.2 improves the result of [10] for separators close to linear functions. In [10] the nonlinear lower bounds for Boolean functions with linear information content have been obtained for separators in $O(m/\log m)$ only. On the other hand the lower bounds of [10] work for unbounded fan-in circuits too, and Hromkovič [10] gives an $\Omega(n^{1/a})$ lower bound for the separators in $O(m^a)$ (e.g. $\Omega(n^2)$ for planar circuits). Theorem 4.2 directly provides the lower bound $\Omega(n^{1+a})$ only for separators in $O(m^a)$. But one can easily derive the higher lower bound $\Omega(n^{1/a})$ from our proof of Theorem 4.2 by showing $z(m) = O(m^a)$ if the separator is in $O(m^a)$.

Acknowledgements

We would like to thank Burkhard Monien for a motivating discussion, Martin Dietzfeldbinger and Friedhelm Meyer auf der Heide for a helpful discussion, as well as Mike Paterson and the referees for their helpful comments and suggestions.

References

[1] A.V. Aho, J.D. Ullman and M. Yannakakis, On notions of information transfer in VLSI circuits, in: *Proc. 15th ACM STOC* (ACM Press, New York, 1983) 133–139.
[2] N. Blum, A Boolean function requiring $3n$ network size, *Theoret. Comput. Sci.* **28** (1984) 337–345.
[3] R.L. Brooks, On coloring the nodes of network, *Proc. Cambridge Philos. Soc.* **37** (1941) 194–197.
[4] Z. Gaber and Z. Galil, Explicit constructions of linear-sized superconcentrators, *J. Comp. System Sci.* **22** (1981) 407–420.
[5] L.H. Harper, W.N. Hsiek and J.E. Savage, A class of Boolean functions with linear combinational complexity, *Theoret. Comput. Sci.* **1** (2) (1975) 161–183.

[6] L.H. Harper, J.E. Savage, Complexity made Simple, in: *Proc. Internat. Symp. on Combinatorial Theory*, Rome (September 1973) 2–15.
[7] J. Hromkovič, The advantages of a new approach to defining the communication complexity of VLSI, *Theoret. Comput. Sci.* **57** (1988) 97–111.
[8] J. Hromkovič, Some complexity aspects of VLSI computations. Part 1. A framework for the study of information transfer in VLSI circuits, *Comput. Artificial Intelligence* **7** (3) (1988) 229–252.
[9] J. Hromkovič, Some complexity aspects of VLSI computations. Part 6. Communication complexity, *Comput. Artificial Intelligence* **8** (3) (1989) 209–225.
[10] J. Hromkovič, Nonlinear lower bounds on the number of processors of circuits with sublinear separators, *Inform. and Comput.* **95** (2) (1991) 117–128.
[11] B.M. Kloss and V.A. Malyshev, Bounds on complexity of some classes of functions, *Vestnik. Moskov. Univ. and Ser. Mat. Mech.* (4) (1965) 44–51 (in Russian).
[12] G. Kumičáková-Jirásková, Chomsky hierarchy and communication complexity, *J. Inform. Process. Cybernet.* **EIK 25** (4) (1989) 157–164.
[13] R.J. Lipton and R. Sedgewick, Lower bounds for VLSI, in: *Proc. ACM STOC'81 (ACM, New York,* 1981) 300–307.
[14] R.J. Lipton and R.E. Tarjan, A separator theorem for planar graphs, *SIAM J. Appl. Math.* **36** (2) (1979) 177–189.
[15] R.J. Lipton and R.E. Tarjan, Applications of a planar separator theorem, *SIAM J. Comput.* **9** (1980) 615–626.
[16] C.A. Ložkin, A.N. Rybko, A.A. Sapoženko, J. Hromkovič and N.A. Škalikova, On a approach to a bound on the area complexity of combinational circuits, in: *Mathematical Problems in Computation Theory, Proc. Banach Center Publications* (Warsaw, 1988) 501–510 (in Russian): extended version: Lower bounds on the area complexity of Boolean functions, *Theoret. Comput. Sci.* **97** (1992) 285–300.
[17] O.B. Lupanov, Ob odnom metode siteza skhem, *zv. VUZ radiofizika* **1** (1958) 120–140 (in Russian).
[18] W.F. McColl, Planar circuits have short specifications, in: *Proc. 2nd STACS'85*, Lecture Notes in Computer Science, Vol. 18 (Springer, Berlin, 1985) 231–242.
[19] W.F. McColl and M.S. Paterson, The planar realization of Boolean functions, *Inform. Process. Lett.* **24** (1987) 165–170.
[20] Ch. Papadimitriou and M. Sipser, Communication complexity, *J. Comput. System Sci.* **28** (1984) 260–269.
[21] W.J. Paul, A $2.5n$- lower bound on the combinational complexity of Boolean functions, *SIAM J. Comput.* **6** (1977) 427–443.
[22] N.P. Redkin, Proof of minimality of circuits consisting of functional elements, *Problemy kibernetiki* **38** (1981) 181–216 (in Russian).
[23] J.E. Savage, Planar circuit complexity and the performance of VLSI algorithms, in: H.T. Kung, R. Sproull, G. Steele, eds., *VLSI Systems and Computations* (Comp. Sci. Press, 1981) 61–67.
[24] G.P. Schnorr, Zwei lineare untere Schranken für die Komplexität Boolescher Funktionen, *Computing* **13** (1974) 155–171.
[25] G.P. Schnorr, A $3n$ lower bound on the network complexity of Boolean functions, *Theoret. Comput. Sci.* **10** (1980) 83–92.
[26] C.E. Shannon, The synthesis of two-terminal switching circuits, *Bell System Techn. J.* **28** (1949) 59–98.
[27] E.P. Sopranenko, Minimal realizations of functions by circuits using functional elements, *Probl. Kibernetiki* **15** (1965) 117–134 (in Russian).
[28] G. Turán, Lower bounds for synchronous circuits and planar circuits, *Inform. Process. Lett.* **30** (1989) 37–40.
[29] J. Ullman, *Computational Aspects of VLSI*, Principles of Computer Science Series (Computer Science Press, Rockville, MD, 1984).
[30] I. Wegener, *The Complexity of Boolean Functions*, Wiley–Teubner Series in Computer Science (Wiley and B.G. Teubner, Stuttgart, 1987).
[31] A.C. Yao, The entropic limitation of VLSI computations, in: *Proc. 13th Annual ACM STOC* (ACM, New York, 1981) 308–311.